

Attorney Docket No. 1046.1309

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Hiroyuki KOMAI

Application No.: To be Assigned

Group Art Unit: To be Assigned

Filed: February 9, 2004

Examiner: To be Assigned

For: AUTHENTICATION INFORMATION PROCESSING METHOD

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-37150

Filed: February 14, 2003

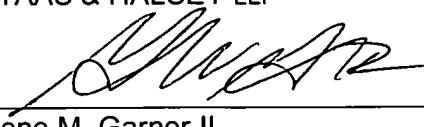
It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Feb. 9, 2004

By:


Gene M. Garner II
Registration No. 34,172

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

OP1710

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2003年 2月14日

出願番号 Application Number: 特願2003-037150

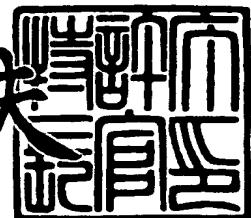
[ST. 10/C]: [JP2003-037150]

出願人 Applicant(s): 富士通株式会社

2003年10月27日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3088648

【書類名】 特許願
【整理番号】 0253366
【提出日】 平成15年 2月14日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/60
【発明の名称】 認証情報処理方法
【請求項の数】 5
【発明者】
【住所又は居所】 東京都稻城市大字大丸1405番地 株式会社富士通パ
ソコンシステムズ内
【氏名】 駒井 広行
【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社
【代理人】
【識別番号】 100089244
【弁理士】
【氏名又は名称】 遠山 勉
【選任した代理人】
【識別番号】 100090516
【弁理士】
【氏名又は名称】 松倉 秀実
【連絡先】 03-3669-6571
【手数料の表示】
【予納台帳番号】 012092
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書 1
【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705606

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証情報処理方法

【特許請求の範囲】

【請求項 1】

ログインを要求するユーザ端末の端末情報を取得するステップと、
前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステッ
プと、

前記ユーザ端末からのログイン操作を受け付けるステップと、
前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ
端末からのログインの可否を判定するステップとを備える、認証情報処理方法。

【請求項 2】

前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶する
ステップをさらに備え、

前記ログイン手順を決定するステップでは、
前記累積ログイン回数に応じて、前記ログイン手順を決定する、請求項 1 に記
載の認証情報処理方法。

【請求項 3】

前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶する
ステップをさらに備え、

前記ログイン手順を決定するステップでは、
前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する
、請求項 1 または 2 に記載の認証情報処理方法。

【請求項 4】

コンピュータに認証情報を処理させる認証情報処理プログラムであり、
ログインを要求するユーザ端末の端末情報を取得するステップと、
前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステッ
プと、
前記ユーザ端末からのログイン操作を受け付けるステップと、
前記前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユ

ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理プログラム。

【請求項 5】

ログインを要求するユーザ端末の端末情報を取得する端末情報取得手段と、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するログイン手順決定手段と、前記ユーザ端末からのログイン操作を受け付けるログイン受付手段と、前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するログイン判定手段と、を有する認証情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は認証情報処理技術に関する。

【0002】

【従来の技術】

一般に、コンピュータ等の各種情報処理装置（以下ユーザ端末とする）からネットワークを介してサーバに接続して運用される各種システム（Webページの利用、各種アプリケーションの利用等を含む）がある。通常、このようなシステムでは、他人による不正利用を防止するために、パスワードやID番号等の認証情報の入力を必要とする。

【0003】

上記システムでは、ユーザ名やパスワード等の個人情報は、サーバ側で一括管理する。そして、ユーザ側は、必要に応じてサーバにログイン（接続）操作をする。ログイン操作を受け付けたサーバは、当該ユーザからのログイン操作の認証処理をする。上記サーバによって、当該ユーザからのログイン操作が認証されると、ユーザは上記システムを利用可能となる。

【0004】

通常、上記認証処理は、ユーザ名或いはパスワード等の認証情報を入力するだ

けで、サーバに接続可能な全ての端末からログインできた。そのため、上記システムでは、サーバへの不正侵入の防止等、セキュリティの確保が十分でなかった。従って、従来のシステムでは、ユーザ情報等の、各種情報漏洩の可能性があった。

【0005】

このような多数のユーザ端末からのログインを受け付けるシステムのセキュリティの維持方法として、例えば以下の方法が挙げられる。

【0006】

まず、ユーザ名或いはパスワード以外の、他の認証情報を入力させるログイン手順も鑑みられている。

【0007】

例えば、上記ログイン手順として、パスワードを入力するものがある。また、他のログイン手順として、キーワード（例：ユーザの個人情報をキーワードとして予め設定しておき、このキーワードを尋ねる）をランダムに表示して、毎回入力する文字を変更するものがある。この他の手順には、指紋認証や個人を特定できるIDカード（スマートカード等）を使用するものがある。さらに、ログイン手順には、ログイン操作のタイミングによってログインを許可するといったものがある。

【0008】

上記のような、ログイン手順の追加によるセキュリティレベルの維持技術以外には、例えば以下の技術が鑑みられている。

【0009】

まず、上記技術として、ログイン時のパスワードを、適時自動的に変更する技術が開示されている（例えば、特許文献1及び特許文献5参照）。

【0010】

また、上記技術として、認証済みのユーザからのログイン操作に対して、次回からの認証を簡易認証で行う、簡易認証に係る技術も開示されている（例えば、特許文献2参照）。

【0011】

さらに、上記技術として、同一のユーザIDを利用する複数の利用者のうち、セキュリティレベルで決まる特定の利用者だけがログインできる、ログイン制御に係る技術も開示されている（例えば、特許文献3参照）。

【0012】

また、上記技術として、ログイン時の通信路のセキュリティレベルを判定して、コマンド実行の可否を判定するログイン方式に係る技術も開示されている（例えば、特許文献4参照）。

【0013】

また、上記技術として、ユーザにより指定されるユーザID及びパスワードと、認証システムにより予め設定されるキー文字列とによる、ユーザ認証に係る技術も開示されている（例えば、特許文献6参照）。

【0014】

【特許文献1】

特開平7-160638号公報

【特許文献2】

特開2000-36809号公報

【特許文献3】

特開平4-277855号公報

【特許文献4】

特開平6-337844号公報

【特許文献5】

特開平7-182064号公報

【特許文献6】

特開2001-273259号公報

【発明が解決しようとする課題】

しかしながら、上記した各種ログイン手順では、不特定の端末から、決められたログイン手順を実行することで、ログインすることができた。従って、上記ログイン手順を解読された場合には、何者かにシステムを不正利用されるおそれがあった。

【0015】

また、自動的にパスワードないしキー文字列を変化させたとしても、正規のユーザを特定する情報はユーザID等であるため、ユーザIDを取得した何者かによつて、不正利用されるおそれがあった。

【0016】

さらに、セキュリティを維持するために多数のログイン手順を設けることは、継続的にシステムを利用するにあたり、正規のユーザの利便性を低下させるおそれがあった。

【0017】

本発明は、前記した事項に鑑みて為されたものであり、ログイン等のユーザ認証のセキュリティと、正規のユーザに対する利便性とを維持することができる、認証情報処理技術を提供することを課題とする。

【0018】**【課題を解決するための手段】**

前記した課題を解決するために、本発明は以下の手段とした。

【0019】

即ち、本発明では、ログインを要求するユーザ端末の端末情報を取得する。そして、本発明は、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定する。また、本発明は、前記ユーザ端末からのログイン操作を受け付ける。そして、本発明では、前記決定したログイン手順と前記受け付けたログイン操作に基づき、前記ユーザ端末からのログインの可否を判定する。

【0020】

本発明では、ログインを要求するユーザ端末を特定して、当該ユーザ端末に対応したログイン手順を決定する。

【0021】

従って、本発明によれば、不特定の端末からのログイン要求を防止するため、不正侵入等に対するシステムの安全性を維持することができる。

【0022】

また、本発明は、前記ユーザ端末からの累積ログイン回数を前記端末情報に関

連付けて記憶してもよい。このとき、本発明では、前記累積ログイン回数に応じて、前記ログイン手順を決定する。

【0023】

従って、本発明によれば、特定のユーザ端末からの正当なログイン回数に応じて、当該ユーザ端末に対するログイン手順を決定するため、正当なログイン操作を継続するユーザのログイン操作を軽減させることができる。

【0024】

また、本発明は、前記ユーザ端末からの最終ログイン時点を前記端末情報に連付けて記憶してもよい。このとき、本発明では、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する。

【0025】

従って、本発明によれば、最終ログイン時点からの経過期間に応じて、前記ユーザ端末のログイン手順を変化させるため、システムの安全性を維持することができる。

【0026】

また、本発明は、以上の何れかの機能を実現させるプログラムであってもよい。また、本発明は、そのようなプログラムをコンピュータが読み取り可能な記憶媒体に記録してもよい。

【0027】

さらに、本発明は、以上の何れかの機能を実現する装置であってもよい。

【発明の実施の形態】

以下、本発明である、認証情報処理方法の一実施の形態について図面を参照して説明する。本実施の形態では、本発明の認証情報処理方法を、実現するために、認証情報処理プログラムを用いる。そして、本実施の形態では、システムを管理するサーバ等の情報処理装置に、この認証情報処理プログラムを導入（インストール）して認証情報処理装置とする。本システムを利用するユーザ側のユーザ端末は、上記認証情報処理装置にログイン（接続）する。認証情報処理装置は、正規のログイン手順を行ったときに、当該ユーザが本システムを利用可能であると判定する。

【0028】

なお、ユーザ端末が認証情報処理装置の本システムにアクセス可能に接続することは、ログオンとも呼ばれ、本発明においてこれらは同等である。

【0029】**〈システム構成〉**

図1は、本発明の認証情報処理方法を実施するシステムの概略構成図である。本システムは、システムを管理する側の認証情報処理装置100と、インターネット或いはLAN (Local Area Network) 等の各種コンピュータネットワークを介して認証情報処理装置100に接続する、正規のユーザ端末200とからなる。また、本システムには、本システムの不正利用を試みる、不正利用者端末300が、上記各種コンピュータネットワークを介して接続している。

【0030】

認証情報処理装置100は、本システムにログインする個々のユーザ端末毎の情報を保持する、管理ファイル101を有する。また、認証情報処理装置100は、ログイン手順及びシステムのセキュリティレベル（不正利用に対する安全性）の情報を関連付けて保持する、セキュリティ定義ファイル102を有する。

【0031】

本実施の形態において、認証情報処理装置100は、ユーザ端末200の端末情報を取得する。認証情報処理装置100は、その端末情報に基づいて、ユーザ端末200のログイン手順を決定する。そして、認証情報処理装置100は、決定したログイン手順によるログイン操作を受け付ける。受け付けたログイン操作が正当なものである場合には、認証情報処理装置100は、このユーザ端末200のログインを許可する。

【0032】**〈ファイル構成〉**

次に、本装置100で認証情報処理を実行する際に参照するファイルの構成について説明する。上記ファイルには、ユーザ毎の情報を保持する、管理ファイル101と、ログイン手順及びセキュリティレベルを関連付けた、セキュリティ定義ファイル102が存在する。

【0033】**〈管理ファイル〉**

図2は、本装置100が保持する管理ファイル101のファイル構成の一例である。管理ファイル101は、ユーザ端末200からのログイン要求とともに端末情報を取得し照合を行うときに、本装置100が参照するファイルである。本装置100には、本システムにログインする個々のユーザ端末200に対応する数のファイルが存在する。

【0034】

図2に示すように、管理ファイル101には、MAC (Media Access Control) アドレス101a、CPU (central processing unit) の型番情報101b、メモリの型番情報101c、最終ログイン日時（本発明の最終ログイン時点の情報）101d、システムへの累積ログイン回数101e、本システムへのログイン失敗回数101f等の、個々のユーザ端末200毎の端末情報が保持されている。

【0035】

ユーザ端末200のMACアドレス101aは、本装置100がユーザ端末200を特定するために用いられる。このMACアドレス101aは、ネットワークに接続する機器にそれぞれ組み込まれて、ネットワークカードに割り当てられている、固有の識別情報である。

【0036】

また、ユーザ端末200に搭載されるCPUの情報101bは、本装置100がユーザ端末200を特定するために用いられる。このCPUの情報101bとしては、例えば、CPUの型番、或いはCPUのクロック周波数等が挙げられる。

【0037】

ユーザ端末200に搭載されるメモリ101cの情報としては、例えば、メモリの型番、或いはメモリの全容量の数値等が挙げられる。

【0038】

また、当該ユーザ端末200からの最終ログイン日時（本発明の最終ログイン

時点の情報) 101dが保持されている。この最終ログイン日時101dに基づいて、本装置100がユーザ端末200のログイン手順を決定する。

【0039】

そして、当該ユーザ端末200のシステムへの累積ログイン回数101eの情報が保持されている。この累積ログイン回数101eに基づいて、本装置100がユーザ端末200のログイン手順を決定する。

【0040】

さらに、管理ファイル101には、本システムへのログイン失敗回数101fの情報が保持されている。このログイン失敗回数101fに基づいて、本装置100がユーザ端末200のログイン手順のレベルを引き上げるか否かを決定する。

【0041】

本装置100は、ユーザ端末200からのログイン要求を受け付けた場合には、当該ユーザ端末200の端末情報を取得する。本装置100は、当該端末情報と、管理ファイル101内のMACアドレス101a、CPU101b、及びメモリ101cの情報を参照し、このマシンがログイン可能なユーザ端末200であるか否かを判定する。

【0042】

当該ユーザ端末200がログイン可能な端末である場合に、本装置100は、以下の処理を行う。

【0043】

本装置100は、当該ユーザ端末200のログイン手順を、最終ログイン日時101dまたは累積ログイン回数101eの情報を参照して、セキュリティ定義ファイル102から索出し決定する。なお、セキュリティ定義ファイル102の詳細な説明については後述する。

【0044】

また、本装置100は、当該ユーザ端末200がログインを失敗する度にログイン失敗回数101fを加算する。本装置100は、このログイン失敗回数101fが一定回数に到達したときに、当該ユーザ端末200からのログイン手順を

変更してセキュリティレベルを強化する。

【0045】

〈セキュリティ定義ファイル〉

図3、図4及び図5は、本装置100が保持するセキュリティ定義ファイル102のファイル構成の一例である。また、図6は、セキュリティレベルをログイン手順と関連付けて保持する、ログイン手順データテーブル102cの一例である。

【0046】

セキュリティ定義ファイル102は、本装置100が累積ログイン回数ないし最終ログイン時点から、ユーザ端末200のログイン手順を決定するためのセキュリティレベルを定義したファイルである。本セキュリティレベルは、その値が大きいほどセキュリティが高いことを示す。

【0047】

図3に示すセキュリティ定義ファイル102aでは、累積ログイン回数とセキュリティレベルとが関連付けて保持される。セキュリティ定義ファイル102aにおいて、例えば、累積ログイン回数が3から5回までであれば、セキュリティレベル4と定義し、累積ログイン回数が11から20回までであれば、セキュリティレベル2と定義する。即ち、本装置100は、当初累積ログイン回数が少ないときには、当該ユーザ端末200のセキュリティレベルを高く設定する。その後、本装置100は、当該ユーザ端末200からの累積ログイン回数が多くなると、対応するセキュリティレベルを引き下げる。なお、本発明において、この累積ログイン回数とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【0048】

また、図4に示すセキュリティ定義ファイル102bでは、最終ログイン時点とセキュリティレベルとが関連付けられて保持される。セキュリティ定義ファイル102bにおいて、例えば、最終ログイン時点からの経過日数が6から10日であれば、セキュリティレベル3と定義し、最終ログイン時点からの経過日数が21日以上であれば、セキュリティレベル5と定義する。即ち、本装置100は

、当該ユーザ端末 200 からの最終ログイン時点からの経過日数が長いときには、対応するセキュリティレベルを引き上げる。また、本装置 100 は、当該ユーザ端末 200 からの最終ログイン時点からの経過日数が短いときには、対応するセキュリティレベルを引き下げる。なお、本発明において、この最終ログイン時点とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【0049】

本実施の形態では、本装置 100 はユーザ端末 200 の累積ログイン回数に該当するセキュリティレベルをセキュリティ定義ファイル 102a から決定する。また、本装置 100 は、最終ログイン時点からの経過日数を、セキュリティ定義ファイル 102b から決定する。そして、本装置 100 は、累積ログイン回数に基づくセキュリティレベルと、最終ログイン時点からの経過日数に基づくセキュリティレベルのうち、セキュリティレベルが高い方を選択してログイン手順に用いる。なお、本発明において、ログイン手順の決定方法は、上述の例に限定されることなく、適宜設定することができる。

【0050】

図 5 に示すセキュリティ定義ファイル 102c では、ログイン失敗回数に応じたセキュリティレベルの変化率の情報が保持されている。セキュリティ定義ファイル 102c において、例えば、ログイン失敗回数が 3 回までであれば、本装置 100 は、セキュリティレベルは現状を維持する。また、ログイン失敗回数が 5 回であれば、本装置 100 は、セキュリティレベルを現状より 2 段階引き上げる。

【0051】

即ち、セキュリティ定義ファイル 102c では、一定の失敗回数に応じてセキュリティレベルの引き上げ幅が定義されている。なお、本発明において、このログイン失敗回数とセキュリティレベルとの対応関係は、本実施の形態に限定されることなく、適宜設定することができる。

【0052】

図 6 に示すログイン手順データテーブル 102d は、本装置 100 がユーザ端

末200に要求するログイン手順を定義するテーブルである。このログイン手順データテーブル102dには、セキュリティレベルに応じたログインの具体的な手順の情報が保持されている。

【0053】

本実施の形態において、例えば、レベル5のログイン手順は、ユーザ名とパスワード入力による認証、キーワードの入力による認証、指紋による認証、スマートカードによる認証、及び所定のボタンを押している時間による認証である。また、レベル3のログイン手順は、ユーザ名とパスワードの入力による認証、キーワードの入力による認証、指紋による認証である。さらに、レベル1のログイン手順では、ユーザ名とパスワードの入力による認証のみである。

【0054】

即ち、ログイン手順データテーブル102dでは、セキュリティレベルに応じて、ログイン手順を軽減させるようにしている。

【0055】

なお、所定のボタンを押している時間による認証は、以下の方法で行う。まず、本装置100側では、ユーザ端末200にあるキーボード上の、予め決められたボタン等を押している時間を予め設定する。そして、本装置100は、ユーザ端末200から、ログイン操作時にボタンを押している時間を取得して、取得した時間と予め設定した時間とを照合する。本装置100は、照合の結果、双方が一致すれば、このユーザ端末200を認証する。

【0056】

本装置100は、このログイン手順データテーブル102dを、セキュリティ定義ファイル102a, 102bのうちセキュリティレベルが高い方と対応させて、ユーザ端末200のログイン手順を決定する。

【0057】

〈ログイン手順による操作例〉

図7から図11は、ログイン時の画面推移図の一例である。図7から図11では、本装置100がセキュリティレベル5のユーザ端末200からのログイン操作を受け付ける場合の画面遷移を示す。

【0058】

まず、システムを使用するユーザは、ユーザ端末200の図示しないディスプレイに表示される図7のログイン手順操作画面1aに対して、ユーザ名及びパスワードを入力する。

【0059】

ユーザ名及びパスワードの認証完了後、本装置100は当該ユーザ端末200に、図8のログイン手順操作画面1bの画面を表示させる。このログイン手順操作画面1bでは、本装置100はユーザのみが知り得る情報を問う。そのため、この情報と、情報を問うための質問とを予め設定する。なお、本実施の形態では、この情報をキーワードと称する。

【0060】

ログイン手順操作画面1bでは、予めサーバ管理者に通知しておいた複数の質問事項のうち、「好きな動物」についての質問が表示される。ユーザは、ユーザ端末200に当該質問のキーワードを入力する。本装置100は、ユーザ端末200から入力されたキーワードを取得する。そして、予め設定したキーワードと、入力されたキーワードとを比較して認証処理を行う。

【0061】

キーワードの認証完了後、本装置100は、ユーザ端末200に図9のログイン手順操作画面1cを表示させる。このログイン手順操作画面1cでは、ユーザ端末200に備えられる図示しない指紋認証システムに、ユーザの指を認識させる。そのため、ユーザ端末200には、不図示の指紋認証装置を備えている。この指紋認証装置として、例えば、スキヤナ等の画像読み取り装置が挙げられる。本装置100は、この指紋の情報をユーザ端末200から取得して認証処理を行う。

【0062】

ユーザ端末200は、指紋認証装置から読みとった指紋データを本装置100に送信する。

【0063】

指紋認証の完了後、本装置100は、ユーザ端末200に図10のログイン手

順操作画面1dを表示させる。ログイン手順操作画面1dでは、ユーザに渡された図示しないスマートカードを、ユーザ端末200に読み込ませる。スマートカードとユーザ端末200との間では、PIN (Personal Identification Number) の照合が行われる。

【0064】

なお、スマートカードとは、CPUやメモリ、或いはセキュリティ回路といったICチップを組み込んだプラスティックカードのことである。なお、スマートカードは、ICカードと称されることもある。このスマートカードの構造、機能は既知のものであるため、詳細な説明を省略する。

【0065】

本装置100において、スマートカードの照合処理に用いた場合、PINの照合処理はスマートカードで行う。スマートカードには、設定した正しいPINが記憶されている。PINの照合処理時には、ユーザ端末200からスマートカードに、入力されたPINが供給される。スマートカードは、入力されたPINを予め設定されているPINと照合する。PINの照合が完了すると、ユーザ端末200は、スマートカードから当該ユーザの認証情報を読み出す。そして、ユーザ端末200は、スマートカードの認証情報を本装置100に送信する。

【0066】

スマートカードによる認証処理完了後、本装置100は、ユーザ端末200に図11のログイン手順操作画面1eを表示させる。ログイン手順操作画面1eでは、ボタンの押し時間による認証が実行される。ユーザは、ユーザ端末200に備えられた不図示のボタンに対して、予め設定されたボタンの押し時間である、所定時間（例えば3秒間）のボタン押しを実行する。本装置100は、このボタンの押し時間が、所定の時間であることを確認して、認証処理を行う。

【0067】

以上の全ての認証処理完了後、ユーザ端末200は、本システムに接続することができる。

【0068】

なお、本実施の形態では、このログイン作業を累積ログイン回数として端末情

報に関連付けて記憶する。このユーザ端末200から正規のログイン手順操作を継続し続けると、本装置100は、当該ユーザ端末200のセキュリティレベルを引き下げて、ログイン手順を簡略化する。

【0069】

例えば、当初セキュリティレベル5であった場合、一定回数正当なログイン操作を継続することで当該ユーザ端末200のセキュリティレベルがレベル4になる。このとき、ユーザ端末200のディスプレイには、ログイン手順操作画面1eの画面が表示されなくなる。更に使用を続けることで、当該ユーザ端末200のセキュリティレベルがレベル3になる。するとログイン手順操作画面1dが省略されて、さらに認証処理が簡素化される。

【0070】

よって、本装置100によれば、セキュリティレベルを維持しつつ、正規のユーザに対する利便性を維持することができる。

【0071】

〈ログイン処理〉

図12は、本装置100によるログイン処理について説明するフローチャートである。本実施の形態における、認証情報処理（ログイン処理）を、図12に基づいて説明する。

【0072】

まず、ユーザ端末200からログイン要求（図12におけるステップ101、以下S101のように省略する）を受け付けた本装置100は、当該ユーザ端末200からの端末情報を取得する。このとき、本装置100は、上記端末情報を基にして、管理ファイル101を検索する。そして、本装置100は、当該ユーザ端末200の最終ログイン時点と累積ログイン回数とを参照する。このとき、本装置100は、双方のセキュリティレベルのうち、セキュリティレベルの高い方（ログイン手順が多い方）を参照する。

【0073】

また、本装置100は、当該ユーザ端末200に関するログイン失敗回数の情報を管理ファイル101より取得する。以上の本装置100による端末情報と管

理ファイル101との照合処理を、ユーザ照合処理とする（S102）。

【0074】

本装置100は、管理ファイル101と関連付けられたセキュリティ定義ファイル102を参照して、当該ユーザ端末200に対する現在のセキュリティレベルを決定する。そして、本装置100は、決定したセキュリティレベルに応じたログイン手順を、セキュリティ定義ファイル102に基づいて決定する（S103）。当該ユーザ端末200に対して決定したログイン手順を通知して、このログイン手順によるログイン操作を、ログイン手順操作画面を介して要求する。

【0075】

ユーザは、本装置100が決定したログイン手順の操作をユーザ端末200に入力する（S104）。本装置100は、ユーザ端末200に入力されたログイン操作を、ネットワークを介して受け付ける。

【0076】

本装置100は、受け付けたログイン操作が正当なログイン操作であるか否かを、セキュリティ定義ファイル102を参照して判定する（S105）。本装置100は、このステップ105の判定の結果、当該ログイン操作が正当なログイン操作である場合には、累積ログイン回数を1回加算する（S106）。そして、本装置100は、当該ユーザ端末200のログインを許可して、認証処理を終了する。

【0077】

上記ステップ105にて、受け付けたログイン操作が正当なログイン操作でないと判定した場合、本装置100は、管理ファイル101のログイン失敗回数を1回加算する（S107）。

【0078】

そして、本装置100は、当該ユーザ端末200のログイン失敗回数が予め設定された一定の回数に到達したか否かを判定する（S108）。このとき当該ログイン失敗回数が一定の回数に到達していない場合には、本装置100は、ユーザ端末200に再度ログイン操作を要求するため、ステップ104の処理に戻る。

【0079】

上記ステップ108の処理において、当該ログイン失敗回数が一定の回数に到達した場合には、本装置100は、セキュリティ定義ファイル102を参照してセキュリティレベルを引き上げる(S109)。そして、本装置100は、ユーザ端末200に再度ログイン操作を要求するため、ステップ104の処理に戻る。

【0080】

このようなログイン処理を行うことによって、本装置100は、セキュリティレベルを維持しつつ、ユーザの利便性を維持することができる。

【0081】**〈実施の形態の効果〉**

本実施の形態では、ログイン時に行う認証方法を、過去の実績から判断し、セキュリティレベルを変動させている。従って、本実施の形態では、従来のユーザ名とパスワードだけのシステムに比べてセキュリティが強固になる。また、本システムは、正当なログイン操作を継続することで当該ユーザ端末200のログイン手順を簡略化するので、常に面倒な入力を行う必要がなくなる。従って、本装置100によれば、ユーザの使い勝手を損なうことなく、不正ログインを防止することができる。

【0082】**〈変形例〉**

なお、本発明の認証情報処理方法は、本実施の形態にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【0083】

例えば、一度不正にログインされた場合、いわゆるハッカーは何度でもそのシステムに侵入することができ、長期的にシステム内の情報を監視できてしまう場合がある。この問題を解決するために、本装置100の処理を簡単なセキュリティレベルから、強固なセキュリティレベルに移行させてもよい。

【0084】

図13は、上記の場合における、ログイン回数が増加するのに応じてセキュリティレベルとログイン手順とを引き上げた、ログイン手順データテーブルの一例である。本処理では、接続回数が多くなればなる程セキュリティのレベルを引き上げる。

【0085】

通常、ハッカー等の不正利用者は、一度ログインに成功すると、同じログイン手順を用いて再度ログイン操作を試みる。本装置100は、一度ログインされた場合であっても、ログイン回数に応じてログイン手順を追加していく。よってハッカーによって何度もログインされる場合に、セキュリティレベルが自動的にあがるため、再侵入を防止することできる。

【0086】

また、本実施の形態において、セキュリティレベルの決定は、当該ユーザ端末200の累積ログイン回数によるセキュリティレベルと、最終ログイン時点からの経過日数によるセキュリティレベルとを参照して、セキュリティレベルが高い方を当該ユーザ端末200のセキュリティレベルと決定した。しかしながら、本発明ではこれに限定されることはない。

【0087】

例えば、累積ログイン回数によって索出されるセキュリティレベルと最終ログイン時点からの経過日数によって索出されるセキュリティレベルのうち、セキュリティレベルの低い方を当該ユーザ端末200のセキュリティレベルと決定してもよい。

【0088】

また、例えば、累積ログイン回数によって索出されるセキュリティレベルと最終ログイン時点からの経過日数によって索出されるセキュリティレベルとの平均値を、当該ユーザ端末200のセキュリティレベルとして決定してもよい。

【0089】

さらに、例えば、累積ログイン回数によって索出されるセキュリティレベルと、最終ログイン時点からの経過日数によって索出されるセキュリティレベルの何れか一方を、当該ユーザ端末200のセキュリティレベルとしてもよい。

【0090】

また、セキュリティレベルを変化させることなく、決定したログイン手順によるログイン操作が正当であった場合に、ユーザ端末200からのログインを許可してもよい。

【0091】

さらに、本装置100は、セキュリティレベルに応じて、ユーザ端末200のアクセス制限を行ってもよい。

【0092】

また、セキュリティレベルに応じて、ログイン時にアクセスできるファイルの範囲を決定する、或いは、接続するファイルの書込制限を行ってもよい。

【0093】

また、セキュリティレベルを索出せずに、累積ログイン回数或いは最終ログイン時点からの経過日数によって、ログイン手順を決定してもよい。

【0094】

また、認証情報は、図2に例示したものに限定されず、端末を識別可能な情報であれば、その種別、或いは利用する個数はいかなるものであってもよい。

【0095】**[その他]**

本発明は、以下のように特定することができる。

【0096】

(付記1) ログインを要求するユーザ端末の端末情報を取得するステップと、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、前記ユーザ端末からのログイン操作を受け付けるステップと、前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理方法。

【0097】

(付記2) 前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記1に記載の

認証情報処理方法。

【0098】

(付記3) 前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記1または2に記載の認証情報処理方法。

【0099】

(付記4) 前記端末情報、前記累積ログイン回数、及び前記経過期間の何れかを参照して、前記ユーザ端末に対するセキュリティレベルを決定するステップをさらに備え、前記ログイン手順を決定するステップでは、前記セキュリティレベルに応じて前記ログイン手順を決定する、付記3に記載の認証情報処理方法。

【0100】

(付記5) ログインを要求するユーザ端末の端末情報を取得する端末情報取得手段と、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するログイン手順決定手段と、前記ユーザ端末からのログイン操作を受け付けるログイン受付手段と、前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するログイン判定手段と、を有する認証情報処理装置。

【0101】

(付記6) 前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶する累積ログイン回数記憶手段をさらに有し、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記5に記載の認証情報処理装置。

【0102】

(付記7) 前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶する最終ログイン時点記憶手段をさらに有し、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記5または6に記載の認証情報処理装置。

【0103】

(付記8) 前記端末情報、前記累積ログイン回数、及び前記経過期間の何れか

を参照して、前記ユーザ端末に対するセキュリティレベルを決定するセキュリティレベル決定手段をさらに有し、

前記ログイン手順決定手段が、

前記セキュリティレベルに応じて、前記ログイン手順を決定する、付記7に記載の認証情報処理装置。

【0104】

(付記9) コンピュータに認証情報を処理させる認証情報処理プログラムであり、ログインを要求するユーザ端末の端末情報を取得するステップと、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定するステップと、前記ユーザ端末からのログイン操作を受け付けるステップと、前記前記決定したログイン手順と前記受け付けたログイン操作に基づき前記ユーザ端末からのログインの可否を判定するステップとを備える、認証情報処理プログラム。

【0105】

(付記10) 前記ユーザ端末からの累積ログイン回数を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記累積ログイン回数に応じて、前記ログイン手順を決定する、付記9に記載の認証情報処理プログラム。

【0106】

(付記11) 前記ユーザ端末からの最終ログイン時点を前記端末情報に関連付けて記憶するステップをさらに備え、前記ログイン手順を決定するステップでは、前記最終ログイン時点からの経過期間に応じて、前記ログイン手順を決定する、付記9または11に記載の認証情報処理プログラム。

【0107】

(付記12) 前記端末情報、前記累積ログイン回数、及び前記経過期間の何れかを参照して、前記ユーザ端末に対するセキュリティレベルを決定するステップをさらに備え、

前記ログイン手順を決定するステップでは、

前記セキュリティレベルを参照してセキュリティレベルを決定する、付記11に記載の認証情報処理プログラム。

【0108】**【発明の効果】**

以上、説明したように本発明の認証情報処理方法によれば、ログインのセキュリティと、正規のユーザに対する利便性とを維持することができるという優れた効果を奏し得る。

【図面の簡単な説明】**【図1】**

本発明の一実施の形態に係る、システムの概略構成図。

【図2】

本実施の形態に係る、認証情報処理装置が保持する管理ファイルのファイル構成の一例。

【図3】

本実施の形態に係る、累積ログイン回数とセキュリティレベルとが関連付けて保持されるセキュリティ定義ファイルの一例。

【図4】

本実施の形態に係る、最終ログイン時点とセキュリティレベルとが関連付けられて保持されるセキュリティ定義ファイルの一例。

【図5】

本実施の形態に係る、ログイン失敗回数とセキュリティレベルとが関連付けられて保持されているセキュリティ定義ファイルの一例。

【図6】

本実施の形態に係る、ログイン手順データーテーブルの一例。

【図7】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図8】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図9】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図10】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図11】

本実施の形態に係る、ログイン時の画面推移図の一例。

【図12】

本実施の形態に係る、本装置によるログイン処理について説明するフローチャート。

【図13】

本実施の形態に係る、ログイン回数が増加するのに応じてセキュリティレベルとログイン手順とを増加させたときの、ログイン手順データテーブルの一例。

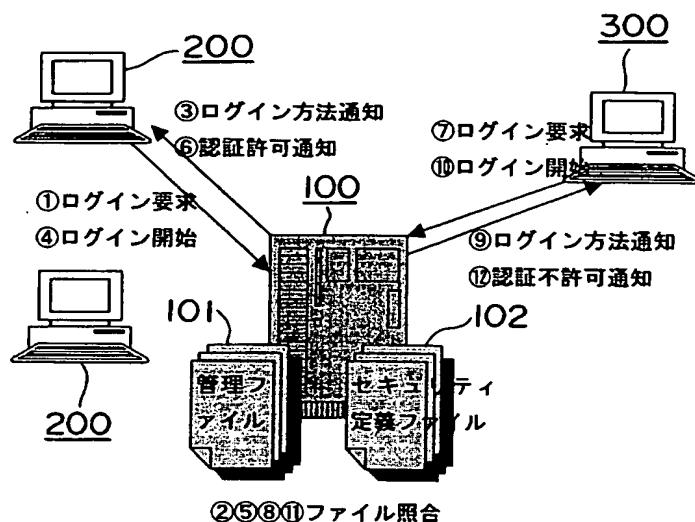
【符号の説明】

- 1 a ログイン手順操作画面
- 1 b ログイン手順操作画面
- 1 c ログイン手順操作画面
- 1 d ログイン手順操作画面
- 1 e ログイン手順操作画面
- 1 0 0 認証情報処理装置
- 1 0 1 管理ファイル
- 1 0 1 a MACアドレス
- 1 0 1 b CPU情報
- 1 0 1 c メモリ情報
- 1 0 1 d 最終ログイン日時情報
- 1 0 1 e 累積ログイン回数情報
- 1 0 1 f ログイン失敗回数情報
- 1 0 2 a セキュリティ定義ファイル
- 1 0 2 b セキュリティ定義ファイル
- 1 0 2 c セキュリティ定義ファイル
- 1 0 2 d ログイン手順データテーブル
- 2 0 0 ユーザ端末
- 3 0 0 不正利用者端末

【書類名】

図面

【図 1】



本発明の一実施の形態に係る、システムの概略構成図

【図2】



【図3】

累ログイン回数	レベル	ログイン手順
1-2	5	レベル5のログイン手順
3-5	4	レベル4のログイン手順
6-10	3	レベル3のログイン手順
11-20	2	レベル2のログイン手順
21	1	レベル1のログイン手順

累積ログイン回数とセキュリティレベルとが
関連付けて保持されるセキュリティ定義ファイル

【図4】

経過日数	レベル	ログイン手順
21-	5	レベル5のログイン方法
11-20	4	レベル4のログイン方法
6-10	3	レベル3のログイン方法
3-5	2	レベル2のログイン方法
1-2	1	レベル1のログイン方法

最終ログイン時点とセキュリティレベルとが
関連付けられて保持されるセキュリティ定義ファイル

【図5】

102c

失敗回数	セキュリティレベル
0 - 3	現状維持
4	現状 + 1
5	現状 + 2
6	現状 + 3
7 -	現状 + 4

ログイン失敗回数とセキュリティレベルとが
関連付けられて保持されているセキュリティ定義ファイル

【図 6】

セキュリティ	ログイン方法	ログイン回数
レベル5	ユーザ名とパスワード入力、キーワード入力、指紋認証 スマートカード、ボタンの押している長さ	1~2
レベル4	ユーザ名とパスワード入力、キーワード入力、指紋認証 スマートカード	3~5
レベル3	ユーザ名とパスワード入力、キーワード入力、指紋認証	6~10
レベル2	ユーザ名とパスワード入力、キーワード入力	11~20
レベル1	ユーザ名とパスワード入力	21以上

ログイン手順データテーブル

【図7】

Io

勤怠管理システム(1/5)	
ユーザー名と、パスワードを入力してください。	
ユーザー名：	<input type="text"/>
パスワード：	<input type="password"/>
<input type="button" value="次へ"/> <input type="button" value="キャンセル"/>	

ログイン時の画面推移図

【図 8】

lb

勤怠管理システム(2/5)

問い合わせに対するキーワードを入力してください。

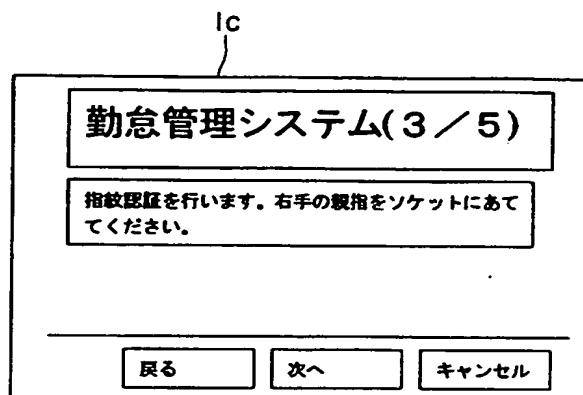
好きな動物は？

キーワード：

戻る 次へ キャンセル

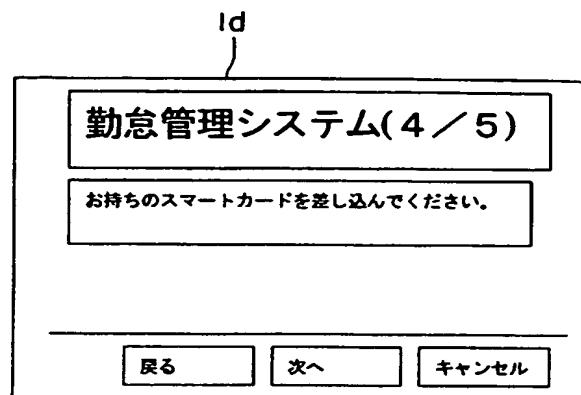
画面推移図

【図9】



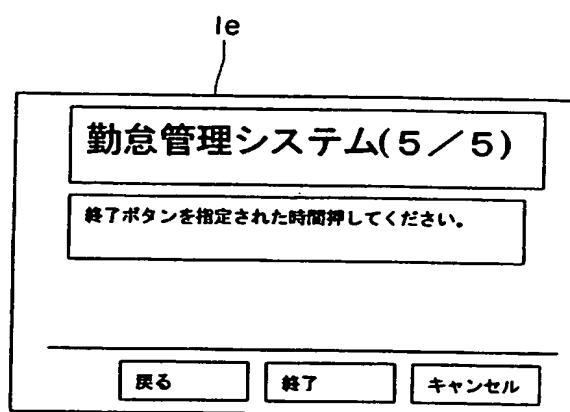
ログイン時の画面推移図

【図10】



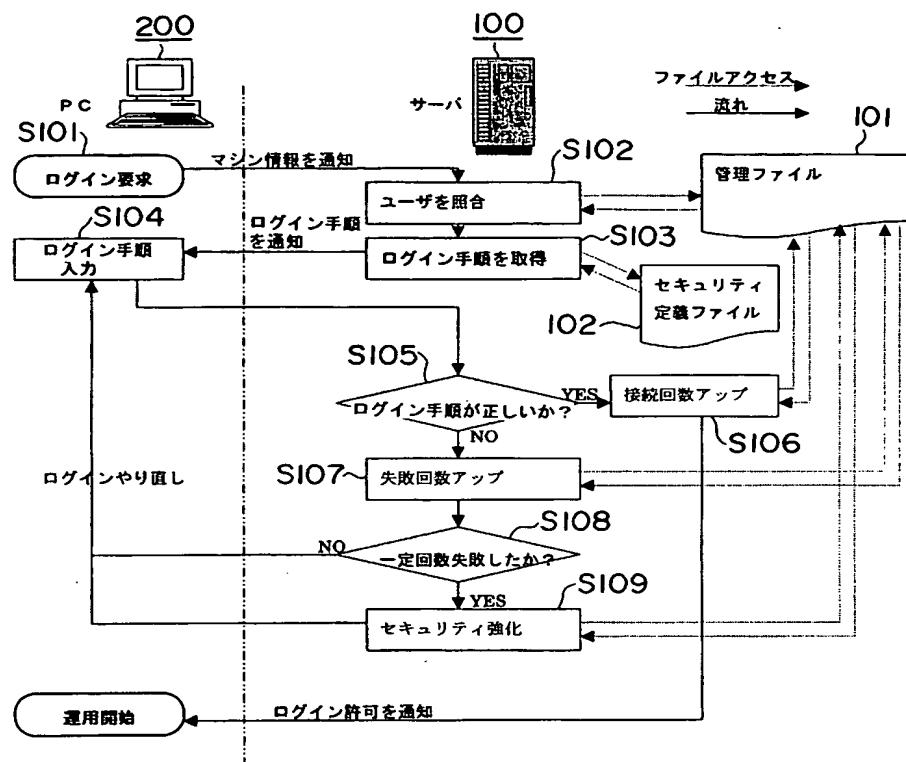
ログイン時の画面推移図

【図11】



ログイン時の画面推移図

【図12】



本実施の形態に係る、本装置によるログイン処理のフローチャート

【図13】

セキュリティ	ログイン方法	ログイン回数
レベル5	ユーザー名とパスワード入力、キーワード入力、指紋認証 スマートカード、ボタンの押している長さ	21回以上
レベル4	ユーザー名とパスワード入力、キーワード入力、指紋認証 スマートカード	11~20
レベル3	ユーザー名とパスワード入力、キーワード入力、指紋認証	6~10
レベル2	ユーザー名とパスワード入力、キーワード入力	3~5
レベル1	ユーザー名とパスワード入力	1~2

ログイン回数が増加するのに応じて
セキュリティレベルとログイン手順とを増加させたときの、
ログイン手順データテーブル

【書類名】 要約書

【要約】

【課題】 ログインのセキュリティと、正規のユーザに対する利便性とを維持することができる、認証情報処理技術を提供する。

【解決手段】 ログインを要求するユーザ端末の端末情報を取得し、前記端末情報に基づき、当該ユーザ端末からのログイン手順を決定し、前記決定したログイン手順によるログイン操作を受け付け、前記ログイン操作が正当である場合に、前記ユーザ端末からのログインを許可する。

【選択図】 図1

特願 2003-037150

出願人履歴情報

識別番号

[000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社